ABSTRACT

The aim of this invention is to pair a security module with one or more host apparatuses in an environment in which the host module has no connection with the management centre.

This aim is achieved thanks to a pairing control method between a first device such as a removable security module and a second device such as a host apparatus, this pairing consisting in securing data exchanges with the aid of a unique pairing key, this method consisting in:

- verifying the pairing between the two devices and using the unique pairing key if the pairing has been already carried out , if not,

- searching for a free location among the locations reserved for the pairing data in the first device and in this case,

- initiating a pairing procedure by transmitting a cryptogram contained in the second device and that contains an identifier belonging to this device, this cryptogram being encrypted by a secret key common to all the first devices,

- decrypting this cryptogram using the first device and extracting from this cryptogram the identifier of the second device,

- generating a pairing key based on this identifier,

- storing in the first device the pairing data with the second device.